⑲日本国特許庁(J.P)　　㉑特許出願公開

⑫公開特許公報(A)　昭63－285661

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和63年(1988)11月22日
G 06 F 15/00		7361－5B	
9/06	330	7361－5B	

審査請求　未請求　発明の数 1　(全5頁)

㊹発明の名称　パスワード切換方式

㉑特　願　昭62－121788
㉒出　願　昭62(1987)5月19日

㉒発明者　山田　正寛　神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア工場内
㉒発明者　石橋　信　神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア工場内
㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
㉔代理人　弁理士　秋田　収喜

明細書

1．発明の名称

パスワード切換方式

2．特許請求の範囲

1．端末装置とホストシステムから構成され、端末装置からホストシステムを使用する際に、端末装置側からホストシステムにパスワードを送出し、ホストシステムがパスワードチェックを行い、この結果により端末装置からのホストシステムの使用許可を与える情報処理システムにおいて、ホストシステムおよび端末装置のそれぞれに、パスワード記憶装置およびパスワード再計算機構を備え、システム使用終了時にホストシステムから端末装置に送出される終了メッセージデータの一部を共通のデータとして、ホストシステム側および端末装置側でそれぞれに次回に使用するパスワードを前記パスワード再計算機構により計算して前記パスワード記憶装置に格納し、次回のパスワードとするパスワード切換方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、パスワード切換方式に関し、詳しくは、システムの不正使用を防止するためにパスワードチェックを行う情報処理システムにおいて、パスワードチェックによるシステム保護をより強固にする方式に関するものである。

〔従来の技術〕

近年、ホストシステムが通信回線、無線通信回線により遠隔の端末装置とが結合されて、利用者が遠隔の端末装置からホストシステムを利用できるようになっている情報処理システムが実用化されている。このような情報処理システムにおいては、端末装置がホストシステムとは離れて設置されており、端末装置の管理が十分に行えないことから、端末装置の使用者を制限することができない。このため、部外者からのシステムの不正使用の防止のために、情報処理システムにパスワードチェックを行うパスワードチェック機構を設けている。このようなパスワードチェック機構は、シ

ステムの使用に先立ち、使用者が端末装置からパスワードを入力し、ホストシステムが予め登録されているパスワードと一致するか否かを判定して、一致がとれれば、ホストシステムの使用許可を与えるようになっているものである。

なお、この種のパスワードチェック機構を用いて、システムの不正使用を防止する技術に関係する公知文献として、特開昭５９－５８５７９号公報がある。

〔発明が解決しようとする問題点〕

ところで、このようなパスワードチェック機構を設けた情報処理システムにおいて、パスワードは、システムの不正使用を防ぐために設けられているものであるが、このパスワードの盗用に関しては配慮されていないものであった。

特に、無線通信回線により端末装置とホストシステムが結合されて、システムを構成している情報処理システムにおいては、無線通信回線を用いているが故に、パスワードが他人に傍受され、パスワードが盗用される可能性が高い。このため、パスワードの盗用にする対策が講じられる必要があるが、従来のパスワードチェック機構を設けた情報処理システムのパスワードチェック方式では、パスワードの盗用による不正使用に関しては、全くの無防備の状態であるという問題点があった。すなわち、無線通信回線を用いてシステムを構成している場合のシステムの安全性に対する配慮がなされておらず、パスワードの盗用、システムの不正使用を起こしやすいという問題点があった。

本発明は、前記問題点を解決するためになされたものである。

本発明の目的は、システムの不正使用を防止するためにパスワードチェックを行う情報処理システムにおいて、パスワードチェックによるシステム保護をより強固にするパスワード切換方式を提供することにある。

本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかになるであろう。

〔問題点を解決するための手段〕

前記の目的を達成するためになされた本発明のうち、代表的なものの概要を簡単に説明すれば、下記のとおりである。

すなわち、端末装置とホストシステムから構成され、端末装置からホストシステムを使用する際に、端末装置側からホストシステムにパスワードを送出し、ホストシステムがパスワードチェックを行い、この結果により端末装置側からのホストシステムの使用許可を与える情報処理システムにおいて、ホストシステムおよび端末装置のそれぞれに、パスワード記憶装置およびパスワード再計算機構を備え、システム使用終了時にホストシステムから端末装置側に送出される終了メッセージを共通のデータとして、ホストシステム側および端末装置側でそれぞれに次回に使用するパスワードをパスワード再計算機構により計算してパスワード記憶装置に格納し、次回のパスワードとすることを主な特徴とする。

〔作用〕

前記手段によれば、パスワード再計算機構が、システム使用終了時にホストシステムから端末装置側に送出される終了メッセージを共通のデータとして、次回使用するパスワードを再計算し、パスワード記憶装置に格納する。このため、ここでは、システム使用毎に、パスワードが再計算されて、パスワードが変更されるので、パスワードが何らかの方法により傍受、盗用されても、システムの不正使用ができなくなり、システムの安全性が高くなる。

ところで、パスワード再計算機構におけるパスワード再計算式は、あらかじめ各ユーザから申請された各ユーザ毎に異った計算式をホストシステム側および端末装置側で登録しておいて用いることにより、ユーザ間でのパスワード盗用も防止することができ、より安全性の高いシステムとすることができる。

〔発明の実施例〕

以下、図面を用いて本発明の一実施例を詳細に説明する。

第１図は、本発明の一実施例のパスワード切換

方式を用いた情報処理システムのシステム構成図である。この情報処理システムは、無線通信回線により端末装置とホストシステムを結合してシステムを構成しており、例えば、このシステムではオンライン処理サービスを提供している。

第1図において、ホストシステムである中央計算機1では、オンライン処理サービスを行う中央側処理装置2が動作しており、端末装置の端末側計算機7および端末装置9等では、無線通信回線用の変復調装置6を介してホストシステムの中央計算機1と接続して、端末装置側からの利用者がホストシステムのオンライン処理サービスを受ける。

利用者が端末装置の端末側計算機7を利用してホストシステムの中央計算機1のオンライン処理サービスを利用する場合、利用者は、まず、端末側計算機7の端末側処理装置8に対して、利用者識別情報を入力し、利用を開始する旨を指示する。端末側処理装置8は、入力された利用者識別情報に基づき、この利用者識別情報に対応してパスワード記憶装置5bに格納してあるパスワードを読み出し、このパスワードと利用者識別情報をホストシステムの中央計算機1に対して送出する。中央計算機1の中央側処理装置2は受け取った利用者識別情報とパスワードを、パスワード記憶装置5aに格納してあるパスワードと利用者識別情報と突き合せて正しい利用者であるかの確認を行い、正しい利用者であれば、中央計算機1の利用を許可し、ホストシステムは当該端末装置に対するオンライン処理サービスを行う。

オンライン処理サービスの利用を終了する時、利用者が端末装置側から中央計算機1に対して終了の旨の指示を行うと、中央側処理装置2は終了メッセージを出力する。この時、中央側処理装置2は同時にこのホストシステム側に設けたパスワード再計算機構3aに対し、終了メッセージのデータを渡して、次回のパスワードを計算するよう指示する。パスワード再計算機構3aは、利用者識別情報に対応して利用者毎にパスワード再計算式記憶装置4aに格納してあるパスワード再計算式を読み出し、終了メッセージのデータを入力データとして、このパスワード再計算式により次回のパスワードを計算する。計算結果の新パスワードは、次回のパスワードとして、パスワード記憶装置5aに利用者識別情報とともに格納する。一方このとき、端末装置側においては、端末側処理装置8が、終了メッセージを受けとると、端末装置側に設けたパスワード再計算機構3bに対し、次回のパスワードを計算するように指示する。端末装置側のパスワード再計算機構3bでは、システム利用開始時に入力された利用者識別情報に対応してパスワード再計算式記憶装置4bに格納しているパスワード再計算式を読み出し、このパスワード再計算式に基づいて、終了メッセージのデータを入力データとして、パスワードを計算する。計算結果の新パスワードは、次回のパスワードとして、パスワード記憶装置5bに格納して、端末装置側からのオンライン処理サービスの利用を終了する。

このように、この実施例のオンライン処理サービスを提供している情報処理システムにおいては、利用者がシステムを使用する毎に、システム使用終了時の終了メッセージを共通のデータとして、次回に使用するパスワードを計算して求め、パスワードの切換を行うようにしている。

第2図は、第1図におけるパスワード再計算機構の概略的な構成を示す機能ブロック図である。

第2図において、パスワード再計算機構3は、パスワード再計算実行機構11とパスワード再計算式入力エリア12からなる。パスワード再計算実行機構11は、処理装置の制御プログラムの指示により、パスワード再計算式記憶装置4に格納されているパスワード再計算式をパスワード再計算式入力エリア12に取り出し、このパスワード再計算式に基づき、パスワードを計算する。ここで用いているパスワード再計算式は、文字データの変換処理を行う関数 $y=S(x)$ および関数 $z=T(y)$ の合関数としている。関数 $y=S(x)$ は、終了メッセージの中から毎回変わる文字列の文字データ、例えば、システムの使用終了時間を表わ

す文字データから、文字列をパスワード長分抜き出す処理を行う関数である。また、関数z=T(y)は、入力の文字列を別の文字列(新パスワード)に変換する処理を行う関数である。パスワード再計算機構3では、このような関数のパスワード再計算式を用いて、パスワードを計算する。得られたパスワードは、次回のパスワードとして、パスワード記憶装置5に格納される。なお、パスワード再計算式を得るための関数y=S(x)および関数z=T(y)は、システムの利用者毎に異なり、このような関数は、システム利用者毎に利用者識別情報と共に予め登録されて、使用者識別情報に対応してパスワード再計算式記憶装置4に格納されているものである。

このように本発明の実施例によれば、システム使用ごとに、パスワードを切り換えるので、第三者が正規システム利用者の通信内容を傍受して識別情報とパスワードを盗用したとしても、次回のパスワードが違うため、システムを利用することができない。関数S(x)および関数T(y)の式はシステム利用者毎に変えることで、無数のパスワード再計算式が得られ、より強固にパスワード保護を行うことができる。

以上、本発明を実施例に基づき具体的に説明したが、本発明は、前記実施例に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることはいうまでもない。

(発明の効果)

以上、説明したように、本発明によれば、システム使用毎にパスワードを毎回変えることができるので、無線通信回線等を用いて構成するシステムのように容易に通信内容を傍受されやすい環境下にあるシステムにおいて、比較的簡単な方法でパスワード保護が可能となり、計算機システムの保全の効果がある。

4. 図面の簡単な説明

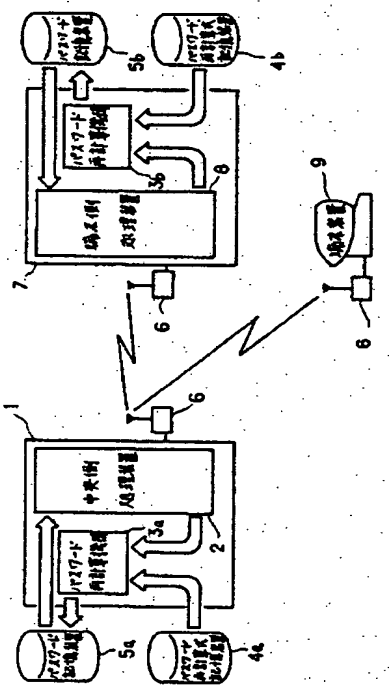
第1図は、本発明の一実施例のパスワード切換方式を用いた情報処理システムのシステム構成図、

第2図は、パスワード再計算機構の概略的な構成を示す機能ブロック図である。

図中、1…中央計算機、2…中央側処理装置、3a,3b…パスワード再計算機構、4a,4b…パスワード再計算式記憶装置、5a,5b…パスワード記憶装置、6…変復調装置、7…端末側計算機、8…端末側処理装置である。

代理人　弁理士　秋田収喜

第1図



第２図